Amendments to the Claims:

Please amend claims 1, 2, 3, 8, 11, 13-15, 17, 19 and 38-42, please cancel claims 21-23, 28-34, 43, 46 and 47 and please add new claims 48-87 as follows.

This listing of claims replaces all prior versions, and listings, of claims in the application.

1. (Currently Amended) A method for preventing unauthorized use of digital content data to be transferred from a first system to a second system comprising:

locating an original archive of a digital content data at the first system;

determining transaction data of the second system that identifies the second system;

~~determining whether the transaction data of the second system indicates whether the second system is a valid recipient of the archive;~~

modifying the original archive using the transaction data of the second system that identifies the second system to generate a modified archive; [[and]]

transferring the modified archive from the first system to the second system ~~if the second system is a valid recipient;~~

receiving the transferred archive at the second system; and

recovering the digital content data of the original archive at the second system using the transaction data of the second system if the second system is a valid recipient.

2. (Currently Amended) The method of claim 1 further comprising, if the second system is not a valid recipient, ~~transferring the archive from the first system to the second system;~~ the operation of the archive failing in the second system.

3. (Currently Amended) The method of claim 1 wherein transferring the modified archive from the first system to the second system comprises transferring the modified archive from the first system to ~~comprises~~ a hard media and transferring the modified archive from the hard media to the second system, and wherein the second system comprises a computer system.

4. (Original) The method of claim 1 wherein the first system comprises a first computer system and wherein the second system comprises a second computer system.

5. (Original) The method of claim 4 wherein the first and second computer systems are remotely located.

6. (Original) The method of claim 1 wherein determining transaction data of the second system comprises determining a data element selected from the group of data elements consisting of: transaction identification; system configuration information; manufacturer, serial number, and physical properties.

7. (Original) The method of claim 1 wherein determining transaction data of the second system comprises downloading an analysis tool to the second system, and running the analysis tool to examine the second system and to generate a unique identifying value that identifies the second system as the transaction data.

8. (Currently Amended) The method of claim 7 wherein the unique identifying value is deposited in the original archive that is transferred to the second system.

9. (Original) The method of claim 8 wherein the unique identifying value is encrypted and interleaved with the digital content data in the transferred archive.

10. (Cancelled)

11. (Currently Amended) The method of claim 1 further comprising increasing a memory allocation of the original archive before modifying the original archive with the transaction data.

12. (Original) The method of claim 11 further comprising creating a map of the increased memory allocation.

13. (Currently Amended) The method of claim 12 further comprising storing the map in the original archive, or in memory locations of the second system, or in the first system.

14. (Currently Amended) The method of claim 1 further comprising, before transferring the modified archive, removing a plurality of original data segments from memory locations of the original archive and storing false data at the memory locations.

15. (Currently Amended) The method of claim 14 further comprising storing the original data in the original archive, or in memory locations of the second system, or in the first system.

16. (Original) The method of claim 15 further comprising generating a map of the memory locations.

17. (Currently Amended) The method of claim 16 further comprising storing the map in the original archive, or in memory locations of the second system, or in the first system.

18. (Original) The method of claim 14 wherein the false data comprises a machine instruction that initiates an abnormal condition in the digital content data when processed.

19. (Currently Amended) The method of claim 14 wherein the second system, following transfer of the modified archive, replaces the false data with the original data segments if the second system is a valid recipient.

20. (Original) The method of claim 19 wherein the second system replaces the false data by the original data segments immediately prior to execution of the corresponding memory locations, and replaces the original data by the false data immediately following execution of the corresponding memory locations.

21.-23. (Cancelled)

24. (Previously Presented) A method for preventing unauthorized use of digital content data hosted on a system comprising:

determining whether an unauthorized use of the digital content data is in progress; and

in the case where an unauthorized use is determined, initiating a defense action by disabling only an input device in association with the unauthorized use, wherein the input device is only disabled in an unauthorized interface window when the target focus for the input device is an unauthorized application associated with the unauthorized interface window.

25. (Original) The method of claim 24 wherein disabling an input device comprises disabling a combination of keystrokes at a keyboard input device.

26. (Original) The method of claim 24 further comprising disabling the input device with regard to user interface windows related to the unauthorized use.

27. (Original) The method of claim 26 wherein the input device comprises a keyboard or a mouse.

28.-34. (Cancelled)

35. (Previously Presented) The method of claim 1 wherein a watermark is deposited in the archive that is transferred to the second system.

36. (Previously Presented) The method of claim 7 wherein the unique identifying value is used to create a system unique encryption key.

37. (Previously Presented) The method of claim 14 wherein the false data comprises a machine instruction which is not properly functional when processed.

38. (Currently Amended) The method of claim 1 further comprising aborting transfer of the

modified archive from the first system to the second system if the second system is an invalid recipient ~~of the archive~~.

39. (Currently Amended) The method of claim 38 wherein the transfer of the modified archive is aborted immediately if the second system is an invalid recipient ~~of the archive~~.

40. (Currently Amended) The method of claim 38 wherein the transfer of the modified archive is aborted in an indirect manner if the second system is an invalid recipient ~~of the archive~~.

41. (Currently Amended) The method of claim 38 further comprising, if it is determined that the second system is an invalid recipient of the original archive, further modifying the original archive to insert executable data into the original archive that causes an exit, an error condition, or communication to another system entity which begins a cascading exit process, in the second system, and transferring the further modified archive to the second system.

42. (Currently Amended) The method of claim 1 further comprising, following the second system receiving the transferred archive, the second system [[and]] de-interleaving or de-crypting the transferred archive using the transaction data of the second system so that the received digital content data can be executed by the second system.

43. (Cancelled)

44. (Cancelled)

45. (Previously Presented) The method of claim 24 further comprising allowing proper function of the input device in an authorized interface window when the target focus for the input device is an authorized application associated with the authorized interface window.

46. (Cancelled)

47. (Cancelled)

48. (New) The method of claim 1 further comprising determining whether the transaction data of the second system indicates whether the second system is a valid recipient of the original archive before transferring the modified archive from the first system to the second system.

49. (New) The method of claim 1 wherein determining transaction data of the second system comprises executing an analysis tool to examine the second system and to generate a unique identifying value that identifies the second system, the transaction data comprising the unique identifying value.

50. (New) The method of claim 49 wherein the analysis tool is executed at a system that is remote to the second system.

51. (New) The method of claim 49 wherein the analysis tool is executed at the second system

52. (New) The method of claim 1 wherein the transaction data of the second system is used to generate a system unique encryption key and wherein modifying the original archive comprises encrypting the original archive using the system unique encryption key to generate the modified archive.

53. (New) The method of claim 52 wherein recovering the digital content data of the original archive comprises decrypting the modified archive at the second system using the system unique encryption key.

54. (New) A method for preventing unauthorized use of digital content data to be transferred from a first system to a second system comprising:

locating an original archive of a digital content data at the first system;

determining transaction data of the second system that identifies the second system by executing an analysis tool to examine components of the second system and to generate a unique identifying value, the unique identifying value identifying the second system and being based on selected properties of the examined components, the transaction data comprising the unique identifying value;

modifying the original archive using the transaction data of the second system that identifies the second system to generate a modified archive; and

transferring the modified archive from the first system to the second system.

55. (New) The method of claim 54 wherein the unique identifying value is deposited in the original archive that is transferred to the second system.

56. (New) The method of claim 55 wherein the unique identifying value is encrypted and interleaved with the digital content data in the transferred archive.

57. (New) The method of claim 54 further comprising downloading the analysis tool to the second system.

58. (New) The method of claim 54 wherein the analysis tool is executed at a system that is remote to the second system.

59. (New) The method of claim 54 wherein the unique identifying value is used to create a system unique encryption key.

60. (New) The method of claim 54 further comprising receiving the transferred archive at the second system and recovering the digital content data of the original archive at the second system using the transaction data of the second system if the second system is a valid recipient.

61. (New)The method of claim 60 wherein the transaction data of the second system is used to generate a system unique encryption key and wherein modifying the original archive

comprises encrypting the original archive using the system unique encryption key to generate the modified archive.

62. (New) The method claim 61 wherein recovering the digital content data of the original archive comprises decrypting the modified archive at the second system using the system unique encryption key.

63. (New) The method of claim 54 further comprising determining whether the transaction data of the second system indicates whether the second system is a valid recipient of the original archive prior to transferring the modified archive from the first system to the second system.

64. (New) The method of claim 54 further comprising determining whether the transaction data of the second system indicates whether the second system is a valid recipient of the original archive following transferring the modified archive from the first system to the second system.

65. (New) The method of claim 54 further comprising determining whether the transaction data of the second system indicates whether the second system is a valid recipient of the original archive both prior to and following transferring the modified archive from the first system to the second system.

66. (New) The method of claim 54 further comprising, determining whether the transaction data of the second system indicates whether the second system is a valid recipient of the archive, and if the second system is not a valid recipient, the operation of the archive failing in the second system.

67. (New) The method of claim 54 wherein transferring the modified archive from the first system to the second system comprises transferring the modified archive from the first system to a hard media and transferring the modified archive from the hard media to the second system, and wherein the second system comprises a computer system.

68. (New) The method of claim 54 wherein the first system comprises a first computer system and wherein the second system comprises a second computer system.

69. (New) The method of claim 68 wherein the first and second computer systems are remotely located.

70. (New) The method of claim 54 wherein determining transaction data of the second system comprises determining a data element selected from the group of data elements consisting of: transaction identification; system configuration information; manufacturer, serial number, and physical properties.

71. (New) The method of claim 54 further comprising increasing a memory allocation of the archive before modifying the original archive using the transaction data.

72. (New) The method of claim 71 further comprising creating a map of the increased memory allocation.

73. (New) The method of claim 72 further comprising storing the map in the original archive, or in memory locations of the second system, or in the first system.

74. (New) The method of claim 54 further comprising, before transferring the modified archive, removing a plurality of original data segments from memory locations of the original archive and storing false data at the memory locations.

75. (New) The method of claim 74 further comprising storing the original data in the original archive, or in memory locations of the second system, or in the first system.

76. (New) The method of claim 75 further comprising generating a map of the memory locations.

77. (New) The method of claim 76 further comprising storing the map in the original archive,

or in memory locations of the second system, or in the first system.

78. (New) The method of claim 74 wherein the false data comprises a machine instruction that initiates an abnormal condition in the digital content data when processed.

79. (New) The method of claim 74 wherein the second system, following transfer of the modified archive, replaces the false data with the original data segments if the second system is a valid recipient.

80. (New) The method of claim 79 wherein the second system replaces the false data by the original data segments immediately prior to execution of the corresponding memory locations, and replaces the original data by the false data immediately following execution of the corresponding memory locations.

81. (New) The method of claim 74 wherein the false data comprises a machine instruction which is not properly functional when processed.

82. (New) The method of claim 54 wherein a watermark is deposited in the archive that is transferred to the second system.

83. (New) The method of claim 54 further comprising aborting transfer of the modified archive from the first system to the second system if the second system is an invalid recipient.

84. (New) The method of claim 83 wherein the transfer of the modified archive is aborted immediately if the second system is an invalid recipient.

85. (New) The method of claim 83 wherein the transfer of the modified archive is aborted in an indirect manner if the second system is an invalid recipient.

86. (New) The method of claim 83 further comprising, if it is determined that the second

system is an invalid recipient of the original archive, further modifying the original archive to insert executable data into the original archive that causes an exit, an error condition, or communication to another system entity which begins a cascading exit process, in the second system, and transferring the further modified archive to the second system.

87. (New) The method of claim 54 further comprising, following the second system receiving the transferred archive, the second system de-interleaving or de-crypting the transferred archive using the transaction data of the second system so that the received digital content data can be executed by the second system.